拒絶引用S01P1115SG00

(12) UK Patent Application (19) GB (11) 2 276 965 (13) A

(43) Date of A Publication 12.10.1994

(21) Application No 9406576.0

(22) Date of Filing 31.03.1994

(30) Priority Data
(31) 931530 (32) 05.04.1993 (33) FI

(71) Applicant(s)
ICL Personal Systems Oy

(Incorporated in Finland)

Kutomotie 18, FIN-00380 Helsinki, Finland

(72) Inventor(s)
Pauli Hovinen

(74) Agent and/or Address for Service
Cruikshank & Fairweather
19 Royal Exchange Square, GLASGOW, G1 3AE,
United Kingdom

(51) INT CL[5]
G06F 12/14

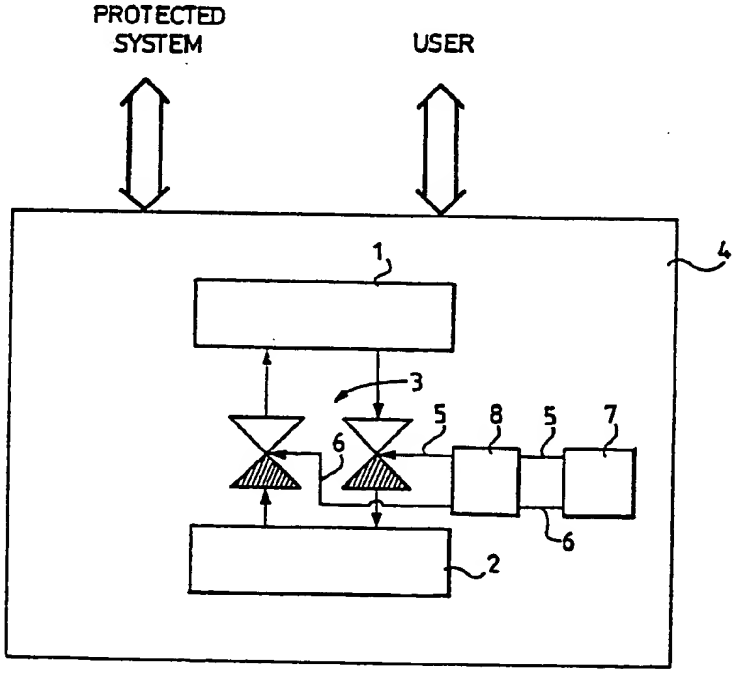
(52) UK CL (Edition M)
G4A AAP

(56) Documents Cited
GB 2247548 A GB 2163577 A

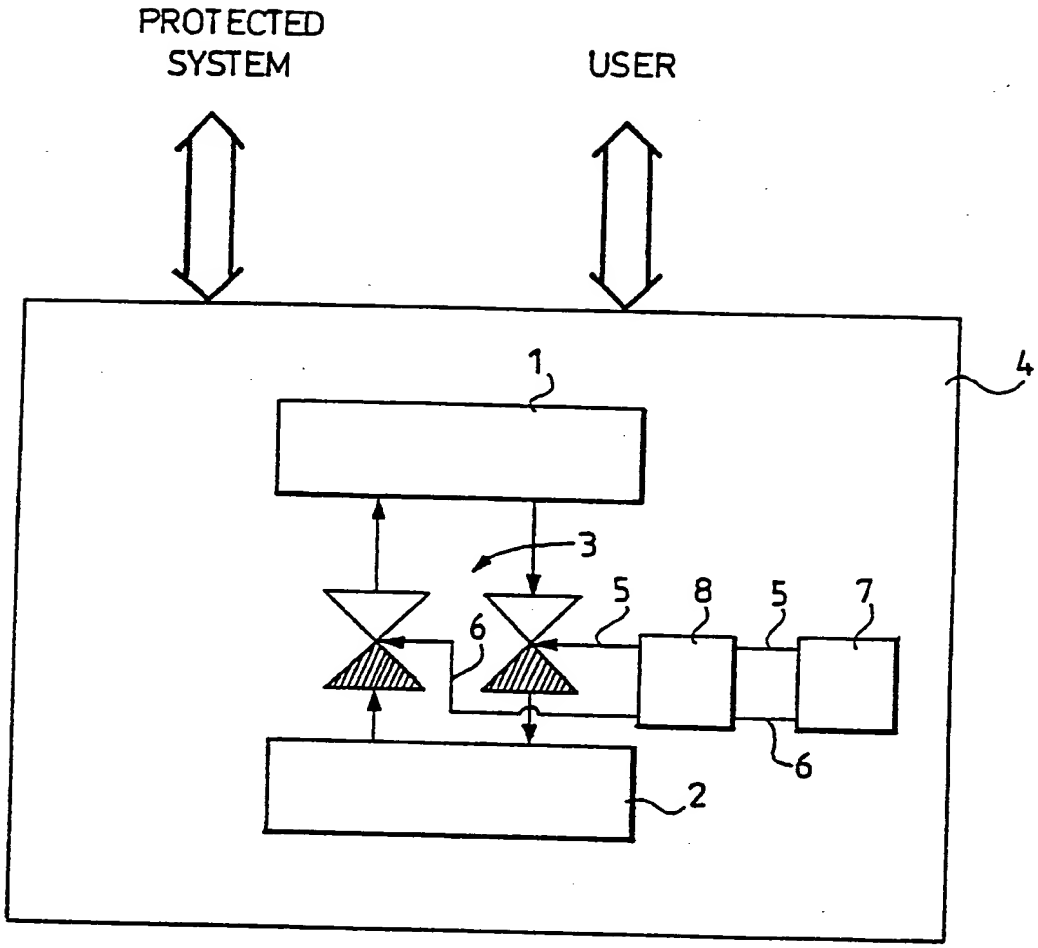
(58) Field of Search
UK CL (Edition M) G4A AAP
INT CL[5] G06F 12/14
ONLINE DATABASES : WPI

(54) Protecting temporarily stored data.

(57) An arrangement for storing data (e.g. swapfiles) in computer equipment (4) comprising a first memory location (1), e.g. a volatile memory, for temporary storage of data for instance for the time of processing, and a second memory location (2), e.g. a non-volatile memory, for longer-term storage of data when desired. Ciphering means (3) converts the data into an encrypted mode with an exchangeable encryption key and into a decrypted mode by a corresponding decryption key. The arrangement also comprises a ciphering key generator (7) for generating at least one random encryption key (5) and a corresponding decryption key (6) for each discrete session. The encryption and decryption keys (5, 6) are retained during a session and their use is prevented after completion of the session, e.g. because they were stored in the volatile memory.



GB 2 276 965 A


PROTECTED SYSTEM
USER
1
4
3
5
8
5
7
6
6
2

AN ARRANGEMENT FOR STORING DATA IN COMPUTER EQUIPMENT

FIELD AND BACKGROUND OF THE INVENTION

The present invention relates to an arrangement for storing data in computer equipment comprising a first memory location, e.g. a volatile memory, for temporary storage of data for instance for the time of processing, and a second memory location, e.g. a non-volatile memory, for longer-term storage of data when desired, and ciphering means for converting the data into an encrypted mode with an encryption key and respectively into a decrypted mode by a decryption key.

Computers make use of non-volatile memories, such as disk memories, for storing data files to be retained only temporarily - e.g. swap files -, since the use of volatile system memories, such as RAM memories, is often costly. Even though temporary data files are retained in a non-volatile memory, they nevertheless are only needed during one session, in other words, during the working period of a user or when computer programs using such data files are run. By a session is meant in this context for example continuous performing of interactive data processing. A session may be contemplated to begin for instance with log-in and to end with log-off. Many computers retain data stored in temporary files in their non-volatile memory. This creates a security problem, since the content of old temporary data files may be retrieved from the non-volatile memory and thus unauthorized persons can access to confidential data possibly stored in such data files. Some computer equipment clear the temporary data files from the non-volatile memory to solve this problem. However, this is of no avail if an attempt is made to read the non-volatile memory before clearing, for instance when the computer has come to an abnormal halt in the midst of a session.

A known method for assuring security is to use ciphering. The data files can be converted into encrypted mode with an encryption program by giving the program an encryption key when the data is written, and the data can be converted into a decrypted mode using the same or another decryption key dependent on the encryption key employed when the data is read. Encryption systems typically require some manner of ciphering key management, to enable safe development, transmission and storage of keys.

It is an object of the present invention to provide a novel arrangement for storing data in computer equipment when data to be retained non-permanently is stored, with which arrangement particularly problems relating to ciphering key management can be substantially eliminated. This is achieved with the arrangement of the invention, comprising a ciphering key generator for generating at least one random encryption key and a corresponding decryption key for each discrete session for use in the cyphering means to encrypt data to be stored non-permanently prior to its storage in the second memory location and respectively to convert it into decrypted mode after reading from the second memory location, and means for retaining the generated encryption and decryption keys during a session and for destroying them after completion of the session at the latest. The basic idea of the invention is that the computer equipment itself generates the encryption and decryption keys that it uses for storing data to be temporarily retained in a non-volatile memory location.

In this way, these encryption and decryption keys are only known to the computer itself. Since the encryption and decryption of data is performed wholly automatically and independently by the computer itself, these operations are fully transparent to the user. However, at the end

of the session at the latest the encryption and decryption keys are destroyed, for example erased from the volatile memory, and thus data possibly stored in the non-volatile memory location and intended only for temporary storage can no longer be deciphered. This procedure assures complete safety even for such temporarily stored data.

The encryption and decryption keys may be generated session-specifically, in which case the same encryption and decryption keys are used for the entire session (these keys may naturally also be the same depending on the ciphering program). Alternatively, encryption and decryption keys may be generated separately for each data file. In cases where several programs are executed during a session, the keys may be destroyed program-specifically, in which event exit from the program causes destroying of the keys.

For a better understanding of the present invention and to show how the same may be carried into effect reference will now be made, by way of example, to the accompanying drawing.

The figure shows at reference 4 computer equipment comprising a volatile memory location 1 which is the memory of the data processing section, such as a volatile memory or processor register. The computer equipment 4 further comprises a second memory location 2 which is a non-volatile memory and provides a storage area for possibly more permanent storing. Typically such a non-volatile memory location is a hard disk. This embodiment specifically relates to safe storage of temporarily stored data or data files in this memory location 2, and thus the figure only concerns storage of such temporarily stored data or data files in said non-volatile memory location 2. For clarity, other storage executed by the computer equipment 4 has not been shown in the figure.

Ciphering means 3 are provided on the data storage and reading route between memory location 1 and memory location 2. Data is stored from memory location 1 to memory location 2 on the one hand and read from memory location 2 to memory location 1 on the other hand through these ciphering means. The encryption and decryption keys 5 and 6 required for these ciphering means 3 are generated by a ciphering key generator 7. This ciphering key generator 7 operates independently and generates the encryption and decryption keys as randomly as possible. These encryption and decryption keys are stored in storage means 8. Generation of the encryption and decryption keys is either session-related, data file-related or application-related. However, it is necessary that the encryption and decryption keys 5 and 6 are retained in storage means 8 only for the time for which the temporary data files or temporarily stored data encrypted by means of them must be available, that is, until the end of the session at the most. Thereafter the data stored using these random ciphering keys in the non-volatile memory location 2 can no longer be deciphered, since the key employed for their encryption has been destroyed from means 8. In practice this can mean for instance that the encryption key and the corresponding decryption key are stored in the volatile memory wherefrom they are lost when power is switched off from the memory circuit in question for instance at the end of a session.

The basic idea of the invention, according to which the encryption and decryption keys must no longer be available after the session, can also be realized in other manners than that contemplated above. The encryption and decryption keys may be selected randomly for example from a large group of alternative keys permanently stored in the microprocessor. In that case, the procedure can be such that the keys can no longer be accessed after the session, even if they existed physically. Also other

methods for storing keys protected in a corresponding manner are possible within the scope of the present invention.

The figure shows as exterior connections interfacing to the computer equipment 4 a user on the one hand and a protected system on the other hand. These are naturally only exemplary user interfaces. The protected system has been indicated as a user interface because by means of the shown computer equipment 4 data temporarily transferred from the protected system for purposes of processing or editing into computer equipment 4 and possibly temporarily stored therein in that connection can be kept protected. This is based on the fact that no decipherable remnants of processed data can remain in the computer equipment 4 after the processing of such protected data therein has been completed.

The arrangement of the invention has been described in the above with reference to one exemplary embodiment, and it is to be understood that equipment-related and computer-related modifications may be made therein without departing from the scope of the invention. A feature of the invention is that, in connection with temporary storage of data, an encryption key known only to the computer itself may be employed and, furthermore, that this key is destroyed by the computer itself or can otherwise no longer be accessed when said temporarily stored data is no longer needed.

CLAIMS

1. A system for storing data in a computer during a computing session and comprising a first memory means suitable for short term storage of data, a second memory means suitable for longer term storage of data, a ciphering key generator for generating at least one random encryption key and at least one corresponding decryption key for the session, ciphering means for converting data read from the first memory means, prior to storage in the second memory means into an encrypted form using the or each encryption key and for converting encrypted data read from the second memory into a decrypted form using the or each decryption key, and means for retaining the encryption and decryption keys during the session and for preventing their use after completion of the session.

2. A system according to claim 1, wherein the first memory means is a volatile memory.

3. A system according to claim 1 or 2, wherein the second memory means is a non-volatile memory.

4. An arrangement for storing data in computer equipment comprising

a first memory location, e.g. a volatile memory, for temporary storage of data for instance for the time of processing;

a second memory location, e.g. a non volatile memory for longer-term storage of data when desired;

ciphering means for converting the data into an encrypted mode with an exchangeable encryption key and into a decrypted mode with a corresponding decryption key, said arrangement comprising

a ciphering key generator for generating at least

one random encryption key and a corresponding decryption key for each discrete session for use in the ciphering means to encrypt data to be stored non-permanently prior to its sotrage in the second memory location and respectively to convert it into decrypted mode after reading from the second memory location; and

means for retaining the generated encryption and decryption keys during a session and for preventing their use after completion of the session.

5. A system for storing data in a computer substantially as hereinbefore described with reference to the accompanying drawing.

Patents Act 1977
Examiner's report to the Comptroller under Section 17
(The Search report)

-8-

Application number
GB 9406576.0

Relevant Technical Fields

(i) UK Cl (Ed.M) G4A AAP

(ii) Int Cl (Ed.5) G06F 12/14

Search Examiner
MR S J PROBERT

Date of completion of Search
10 JUNE 1994

Databases (see below)
(i) UK Patent Office collections of GB, EP, WO and US patent specifications.

(ii) ONLINE: WPI

Documents considered relevant following a search in respect of Claims :-
1-5

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family; corresponding document.

Category	Identity of document and relevant passages		Relevant to claim(s)
A	GB 2247548 A	(GEC MARCONI) see abstract	1-5
A	GB 2163577 A	(N.R.D.C.) see page 1	1-5

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).